ARTICLE APPEARED ON PAGE 1
BUSINESS SECTION

WASHINGTON POST
22 April 1985

Top-Secret Program Boon To Area Firms

Aims to Shield Data From Eavesdroppers

By Michael Schrage
Washington Post Staff Writer

Shrouded in the darkest cloaks of classification, America's national security establishment is pouring more than a billion dollars a year into a special program to prevent the government's computers from leaking their secrets.

The program is known as Tempest, and it has proved to be a multimillion-dollar bonanza for a growing list of defense contractors specializing in the arcane craft of muting the electric squeals and whispers of computers.

"Over the last five years, Tempest has taken quantum leaps, quantum leaps," said Win Tuck, president of Inteq. A leading Tempest contractor, Inteq, based in Herndon, has revenue in excess of $20 million a year. "Based on what we've seen, over the next two years, our revenue will go up by an order of magnitude," he said. That kind of rapid growth is possible because even the most sophisticated computers just can't keep a secret. Lurking within their smooth metal, wires and circuitry is the physics of betrayal.

Just as a skilled mechanic can figure out what is wrong with a car engine by hearing it run, a talented electronic eavesdropper can listen to the inner workings of a computer. Precisely because they are electronic devices, computers can't help leaking radio waves into the air as they compute. With antennae sensitive enough and the right equipment, national security technologists fear, foreign agents could eavesdrop on those radio emissions to find out exactly what is going on in government computers. So those machines must be specially shielded—or "Tempested," in the language of the industry—to prevent them from leaking. What is more, because computer screens, cables, printers and other peripheral devices also broadcast radio-wave frequencies, they have to be Tempest-protected as well.

The result is a thriving defense industry now reaching new levels of profitability as personal computers pour into the national security establishment and the Reagan administration presses harder for more secure computer systems. The Pentagon, each of the armed services, the Central Intelligence Agency and top defense contractors handling sensitive data all are increasingly being required to store their information in computer systems that meet the rigorous Tempest specifications. The driving force behind the Tempest boom is the nation's largest and possibly most secret intelligence organization—the National Security Agency.

Historically, the NSA has been responsible for monitoring, identifying, intercepting and decoding sensitive communications. Reportedly, the agency has acres and acres of huge antennae and supersophisticated computers at its Fort Meade site to accomplish its mission.

But the agency also is responsible for making sure America's own national security communications are safe from foreign interception. Hence, its intense and growing interest in Tempest.

To assure that there would be an adequate supply of Tempest equipment, the NSA set up the Industrial Tempest Program in the late 1970s to let the computer community know what Tempest was and how to meet its security standards. After an initially slow start (the NSA was unused to working with the private sector, sources indicated), ITP has become "very much a dynamic program that seems to be advancing greatly," said one top NSA Tempest official who spoke on the condition that he not be identified.

The NSA "doesn't promise [private computer firms] any particular market," said the official, but it will promise to "support them in a number of technical and administrative ways.

"In the last few years, we've gone from a handful of people and products to over 134 participating companies and more than 270 on the [NSA's] Preferred Product List [for Tempest-approved equipment]," he said.

Participants include some of the biggest names in the computer industry—including IBM, Digital Equipment Corp. and Wang Laboratories. They also include a host of smaller companies—Tempest boutiques—such as Inteq and Systematics General of Sterling, which specialize in making ordinary computer systems Tempest-secure. Inteq and Systematics General are two of the leaders in applying Tempest technology to computers and related equipment. MBI Business Centers Inc. (formerly The Math Box Inc.) of Rockville currently runs the only Tempest personal computer store in Arlington, selling only to consumers with the appropriate clearance.

"Bringing a product to the Tempest market is analogous to remodeling a house," said Gene Mitchell, the Tempest product manager for Delta Data Systems, a Pennsylvania-based Tempest company with facilities in Reston.

But remodeling—or retrofitting—an existing commercial computer to meet Tempest standards is very expensive. The NSA official estimates that there is a Tempest "premium that is extremely costly—anywhere from a 100 percent to a 300 percent premium" involved in turning an ordinary $3,500 personal computer into the equivalent of a $10,000 one.

Indeed, one of the reasons the NSA set up the industrial Tempest program was to encourage manufacturers to gain economies of scale by producing Tempest equipment in volume. This was to help reduce the far more expensive practice of buying commercial machines and retrofitting them. Either way, companies that meet the Tempest standards and win government contracts stand to make a healthy return on their national security technology investments.

"We're very satisfied with the growth rate we're experiencing," said Dick Nichols, the senior product manager for secure systems for Wang Laboratories, which has more items on the NSA's Preferred Products List than any other company. "We're growing faster than the corporation as a whole. Its margins are better and it certainly is, in general, a better business than the computer business as a whole. It doesn't hurt to have the sure, steady flow of government business."

Continued

Systematics General President Bernard Farkas reports that his company's growth in the Tempest market comfortably exceeds 35 percent a year. Other Tempest contractors are enjoying similar growth.

In many ways, the Tempest realm is arguably one of the coziest niche businesses available to a high-technology company. It enjoys both high growth and high margins, and—unlike the commercial computer market—it is free from the specter of Japanese competition. National security restrictions preclude foreign companies from competing.

But while Tempest contractors will cheerfully discuss their finances, they become as quiet as a Tempest computer when technology is the topic. Fundamentally, though, the thrust of Tempest is to prevent radio-frequency emissions from traveling beyond the computer. The most obvious technology to accomplish that is to wrap a copper sheath and gaskets around the computer system like a giant can. Indeed, some companies prosper in the Tempest market by creating copper-lined Tempest rooms for large computer systems.

Another approach, fast gaining popularity, is the use of "elastomers"—conductive plastics—and electrically conductive paints that absorb radio emission. They create a more aesthetically appealing form of protection than the unwieldy metal box.

There is also an opportunity for some software trickery. A special computer chip built into a Tempest computer or peripheral could generate a computer program that runs simultaneously with the program the computer is actually running. This concurrent program could generate enough "noise" to effectively scramble any signal the eavesdropper might manage to pick up. Such software scrambling is particularly intriguing because the NSA has discovered that some of the more traditional forms of Tempest shielding erode over time.

However, because of the extraordinarily sensitive nature of Tempest technology, the NSA and its contractors do not discuss how it can or should be implemented.

Tempest technology is not likely to stop at national security. There is growing sentiment that it has commercial applications.

"Tempest is a hot technology right now," said Donn Parker, a computer security consultant with California's SRI International, adding that defense contractors and high-technology companies in Silicon Valley are exploring whether or not their computer systems need Tempest protection. In fact, he said, there are firms afraid that both the Soviet Union *and* the Japanese are eavesdropping on their computers.

One Dutch computer security expert is encouraging banks to offer Tempest equipment to make sure that criminals cannot pick up home-banking passwords and illegally tap into the bank computer to withdraw funds.

"I think [commercial] Tempest is going to be a big item in the future," said the NSA official. "It's already a topic of discussion. We have had contact with some of our ITP people for the express purpose of dealing with the private sector, if you will." But for now, the NSA official said, "It's really remarkable seeing all this activity going on. I didn't realize that the government marketplace was big enough to support all this activity." ■